PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-106470
(43)Date of publication of application : 22.04.1997

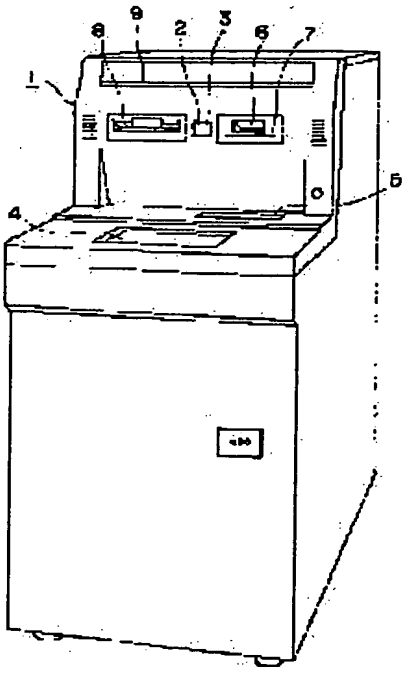
(51)Int.CI. G07D 9/00
G06F 15/00
G06F 19/00
G06T 7/00

(21)Application number : 07-262737
(22)Date of filing : 11.10.1995

(71)Applicant : OKI ELECTRIC IND CO LTD
(72)Inventor : MORI TORU
SUDO SHINICHI

(54) AUTOMATIC TRANSACTION SYSTEM AND INDIVIDUAL IDENTIFICATION METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent illegal transaction processing by excluding a doubtful person by providing an attention calling means for calling the attention of a handling person when the handling person wears sunglasses.
SOLUTION: An automatic teller machine(ATM) 1 can not sample iris data sometimes. When the handling person wears the sunglasses, for example, a display (display input part) 4 is made dark so that the handling person may put off the subglasses unconsciously. Besides, a message such as 'Please put off your sunglasses' is displayed on the display input part 4 so that the handling person may put off the sunglasses positively. Further, when the handling person wear a patch on his/her eye, transaction processing can be performed by a personal identification number but transaction processing requiring high security is disabled. Then, the iris data of an eye not covered with the patch are stored in a transaction data recording part and when any illegal transaction processing is generated, it is proved that transaction processing is not transaction processing due to the customer himself/herself.



LEGAL STATUS

[Date of request for examination] 29.11.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－106470

(43)公開日　平成９年(1997)４月22日

(51)Int.Cl.⁶		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０７Ｄ	9/00	４６１		Ｇ０７Ｄ	9/00	４６１Ａ
Ｇ０６Ｆ	15/00	３３０		Ｇ０６Ｆ	15/00	３３０Ｆ
	19/00				15/30	３３０
Ｇ０６Ｔ	7/00					３４０
					15/62	４６５Ｋ

審査請求　未請求　請求項の数10　ＯＬ　（全 13 頁）

(21)出願番号　特願平7－262737

(22)出願日　平成７年(1995)10月11日

(71)出願人　000000295
沖電気工業株式会社
東京都港区虎ノ門１丁目７番12号

(72)発明者　森　亨
東京都港区虎ノ門１丁目７番12号　沖電気工業株式会社内

(72)発明者　須藤　伸一
東京都港区虎ノ門１丁目７番12号　沖電気工業株式会社内

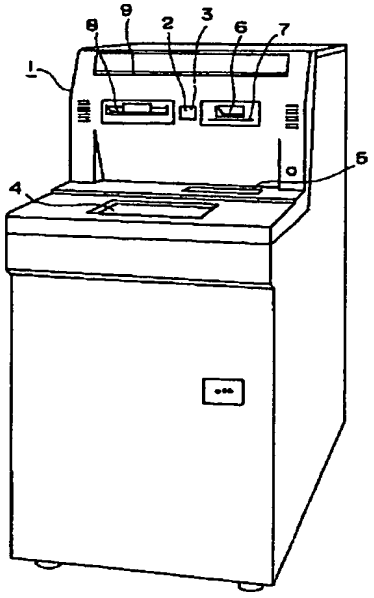
(74)代理人　弁理士　大西　健治

(54)【発明の名称】　自動取引システムおよび個人識別方法

(57)【要約】

【課題】目の表層側のパターンから抽出される虹彩データを用いて個人識別を行う際に、どのようにして個人識別に用いられる顔・目のデータを良好に採取するかを課題とする。

【解決手段】自動取引システムは、取扱者がサングラスをしているのか否かを識別するサングラス識別手段と、サングラス識別手段がサングラスを識別した場合には、取扱者に注意を喚起する注意喚起手段とを有する構成とした。前記注意喚起手段は、表示の輝度を変化する構成、またはサングラスを外すように誘導表示する構成とした。また自動取引システムは、採取した顔・目のデータから取扱者が眼帯をしているのか否かを識別する眼帯識別手段を有し、眼帯識別手段があらかじめ個人識別用に登録されている方の目に眼帯を識別した場合には、採取した目のデータを用いて個人識別を行わない代わりに、暗証番号を用いた個人識別を行うとともに、他方の目のデータを採取して記録する構成とした。



本発明に係る金融端末装置の一例を示す図

【特許請求の範囲】
【請求項１】　取扱者の顔・目のデータを採取し、採取した目のデータを用いて個人識別を行う自動取引システムにおいて、
採取した顔・目のデータから取扱者がサングラスをしているのか否かを識別するサングラス識別手段と、
前記サングラス識別手段がサングラスを識別した場合には、取扱者に注意を喚起する注意喚起手段とを有することを特徴とする自動取引システム。
【請求項２】　前記注意喚起手段は表示の輝度を変化することを特徴とする請求項１記載の自動取引システム。
【請求項３】　前記注意喚起手段は表示の輝度を落とすことを特徴とする請求項２記載の自動取引システム。
【請求項４】　前記注意喚起手段はサングラスを外すように誘導表示することを特徴とする請求項１記載の自動取引システム。
【請求項５】　取扱者の顔・目のデータを採取し、採取した目のデータを用いて個人識別を行う自動取引システムにおいて、
採取した顔・目のデータから取扱者が眼帯をしているのか否かを識別する眼帯識別手段とを有し、
前記眼帯識別手段があらかじめ個人識別用に登録されている方の目に眼帯を識別した場合には、採取した目のデータを用いて個人識別を行わない代わりに、暗証番号を用いた個人識別を行うとともに、他方の目のデータを採取して記録することを特徴とする自動取引システム。
【請求項６】　採取した目のデータを用いて個人識別を行う個人識別方法において、
あらかじめ個人識別する側の目のデータを登録しておき、個人識別する際に登録した側の目にサングラスをしているのか否かを識別し、サングラスをしている場合には、取扱者に注意を喚起することを特徴とする個人識別方法。
【請求項７】　注意の喚起は表示の輝度を変化することによって行うことを特徴とする請求項６記載の個人識別方法。
【請求項８】　注意の喚起は表示の輝度を落とすことによって行うことを特徴とする請求項７記載の個人識別方法。
【請求項９】　注意の喚起はサングラスを外すように誘導表示することによって行うことを特徴とする請求項６記載の個人識別方法。
【請求項１０】　採取した目のデータを用いて個人識別を行う個人識別方法において、
あらかじめ個人識別する側の目のデータを登録しておき、個人識別する際に登録した側の目に眼帯をしているのか否かを識別し、眼帯をしている場合には、採取した目のデータを用いて個人識別を行わない代わりに、暗証番号を用いた個人識別を行うとともに、他方の目のデータを採取して記録することを特徴とする個人識別方法。

【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、虹彩データを用いた金融端末装置および金融システムならびに個人識別方法に関するものである。
【０００２】
【従来の技術】近年、金融機関ではサービスの高度化、多様化が進められてきた。それに伴い、セキュリティの高い装置が求められるようになってきた。「セキュリティの高い」とは、個人を識別する能力が高いとともに、個人識別に用いられるデータが盗用される危険が少なく、安全性の高いことを意味する。従来、このような装置として、例えば、のぞき穴の奥に配設された電子カメラが取扱者の網膜データを採取して、あらかじめ記録している網膜データと照合して個人識別を行う装置が提案された。
【０００３】
【発明が解決しようとする課題】従来、提案された網膜データを用いた装置は、のぞき穴に目を接眼させて網膜データを採取する構成となっていた。それは網膜が目の奥底にあるので、暗くした状態で目の奥底に光を照射して網膜を鮮明にしなければ、良好な網膜データが採取できないからである。そのため、この装置は、取扱者にのぞき穴をのぞき込むという特別な動作を強いることになっていた。また、のぞき穴に目を接眼させるので、不衛生であった。その結果、この個人識別は取扱者に煩わしさを感じさせたり、不快感を感じさせたりするという欠点を有していた。本発明では、目の表層側のパターンから抽出される虹彩データを用いて個人識別を行うことによりこのような欠点を解消し、その際に、どのようにして個人識別に用いられる顔・目のデータを良好に採取するかを課題とする。
【０００４】
【課題を解決するための手段】第１の発明は、取扱者の顔・目のデータを採取し、採取した目のデータを用いて個人識別を行う自動取引システムを、採取した顔・目のデータから取扱者がサングラスをしているのか否かを識別するサングラス識別手段と、サングラス識別手段がサングラスを識別した場合には、取扱者に注意を喚起する注意喚起手段とを有する構成とした。
【０００５】第２の発明は、第１の発明の注意喚起手段を、表示の輝度を変化することを特徴とする構成とした。
【０００６】第３の発明は、第２の発明の注意喚起手段を、表示の輝度を落とすことを特徴とする構成とした。
【０００７】第４の発明は、第１の発明の注意喚起手段を、サングラスを外すように誘導表示することを特徴とする構成とした。
【０００８】第５の発明は、取扱者の顔・目のデータを採取し、採取した目のデータを用いて個人識別を行う自

動取引システムを、採取した顔・目のデータから取扱者が眼帯をしているのか否かを識別する眼帯識別手段とを有し、眼帯識別手段があらかじめ個人識別用に登録されている方の目に眼帯を識別した場合には、採取した目のデータを用いて個人識別を行わない代わりに、暗証番号を用いた個人識別を行うとともに、他方の目のデータを採取して記録する構成とした。

【０００９】第６の発明は、採取した目のデータを用いて個人識別を行う個人識別方法を、あらかじめ個人識別する側の目のデータを登録しておき、個人識別する際に登録した側の目にサングラスをしているのか否かを識別し、サングラスをしている場合には、取扱者に注意を喚起することとする。

【００１０】第７の発明は、第６の発明の注意の喚起を、表示の輝度を変化することによって行うこととする。

【００１１】第８の発明は、第７の発明の注意の喚起を、表示の輝度を落とすことによって行うこととする。

【００１２】第９の発明は、第６の発明の注意の喚起を、サングラスを外すように誘導表示することによって行うこととする。

【００１３】第１０の発明は、採取した目のデータを用いて個人識別を行う個人識別方法を、あらかじめ個人識別する側の目のデータを登録しておき、個人識別する際に登録した側の目に眼帯をしているのか否かを識別し、眼帯をしている場合には、採取した目のデータを用いて個人識別を行わない代わりに、暗証番号を用いた個人識別を行うとともに、他方の目のデータを採取して記録することとする。

【００１４】

【発明の実施の形態】個人識別は、セキュリティが高く、かつ取扱者（通常は口座を開設した顧客自身）に煩わしさや不快感を与えることなく行い得ることが望まれる。つまり、個人を識別する能力が高く、また個人識別に用いられるデータが盗用される危険が少なく、安全性の高いとともに、取扱者が特別な動作をしなくても個人を識別するためのデータを入力できることが望まれる。本発明では、このような条件を満たすために、目の表層側のパターン、特に虹彩のパターンを用いたデータを扱うことにする。

【００１５】前記の虹彩には、水晶体を中心に放射状の黒い筋や外周の輪郭などのパターンが形成されている。このパターンは、人の幼年期に固定されるものであり、個人毎に、また同一人物であっても右目と左目で異なるものである。そのため、このパターンを用いたデータは個人識別能力が非常に高いデータとなる。そこで、このパターンを所定の線に沿って光学的な走査を行い、その走査によって抽出された明暗をデジタル符号化する。このデジタル符号化されたデータ（以下、虹彩データと称する）は、上述の通り個人識別能力が非常に高いデータとなる。しかも、他人が知り得ても盗用できないので安全性の高いデータとなる。また虹彩データは目の表層側のパターンから抽出される。そのため虹彩データは、取扱者に特別な動作を強いることなく、カメラが一定距離離れた位置から採取した目のデータから抽出され得る。さらに虹彩データは、取扱者が目をのぞき穴に接眼する必要がなく採取された目のデータから抽出される。そのため虹彩データは清潔な状態で抽出される。したがって、虹彩データを用いた個人識別は、セキュリティが高く、また、取扱者に煩わしさを感じさせないとともに不快感を感じさせない方法となる。

【００１６】本発明は、このような虹彩データを用いた自動取引システム（金融端末装置やホストコンピュータ、その他周辺機器の各単体装置またはこれらを組み合わせたもの）および個人識別方法を提供するものであり、特に、取扱者が特別な動作をしなくてもこの虹彩データを良好に抽出できるように工夫したものである。また、本発明は、金融機関が速やかに導入できることを意図して、現行の暗証番号を用いた個人識別を行う自動取引システムと組み合わせて運用できるように工夫したものである。

【００１７】以下に、図面を用いて本発明を説明する。図１は本発明に係る金融端末装置の一例を示す図である。図２は本発明に係る金融端末装置の他の例を示す図である。図３は本発明に係る金融端末装置の内部ブロックを示す図である。なお、図中の金融端末装置は自動取引装置（ＡＴＭ）を一例として示しているが、この他にも現金支払機（ＣＤ）、窓口装置、印鑑照会機、証書発行機などの形態がある。

【００１８】図１および図２中、１は金融端末装置（ＡＴＭ）であり、２は近接センサ、３はカメラ、４は表示入力部、５は紙幣挿入・排出口、６はカード挿入・排出口、７は伝票排出口、８は通帳挿入・排出口、９は照明部である。

【００１９】図３中、１０はターミナルコントローラーであり、１１はホストコンピュータ、１２はカメラ制御部、１３は表示制御部、１４は入力制御部、１５は紙幣取扱部、１６はカード取扱部、１７は伝票取扱部、１８は通帳取扱部、１９は主制御部、２０は主記録部、２１は取引データ記録部、２２はカードである。

【００２０】ＡＴＭ１は、ターミナルコントローラー１０を介してオンラインでホストコンピュータ１１と接続されており、取扱者によって各種取引処理の指示が入力されることによりホストコンピュータ１１と通信を行う。これによって各種取引処理が実行される。

【００２１】近接センサ２は、赤外線や超音波を用いて人体が近付いたことを検知するセンサである。近接センサ２は、ＡＴＭ１の前面にパネルによって隠蔽されて配設されている。近接センサ２は、特に、超音波を用いた場合には、人体が近付いたことのみならず、人体までの

距離をも検知することができる。また人体から反射するエコーによって人体のプロポーションを割り出すことができるので、顔の輪郭も識別することができる。

【００２２】カメラ３は、取扱者の顔・目のデータを採取する入力部である。カメラ３は、カメラ制御部１２（または主制御部１９）の制御によって焦点や採取感度を変えることができる。カメラ３は、図１のようにＡＴＭ１の前面に配設される場合と、図２のように表示入力部４の近傍に配設される場合が考えられる。図１の場合は、取扱者がＡＴＭ１に近付いてくる際にデータを採取するのに都合が良い。また図２の場合は、取扱者が表示入力部４に視線を注視するので、取引処理中にデータを採取するのに都合が良い。このカメラ３を制御するカメラ制御部１２（または主制御部１９）は、上述の通りカメラ３の焦点や採取感度を制御しているが、これ以外に、取扱者の顔・目のデータから虹彩データを抽出したり、サングラスや眼帯を抽出したりする。

【００２３】なお、カメラ３は以下のように構成することができる。

【００２４】カメラ３は、周囲の動画データを採取して、数フレーム前後の動画データ同士を比較する。これによって周囲の動画データの中から変化を伴う部分を検知する。このような部分を検知すると、その部分の形状と人体の形状とを比較して、人体の形状に近いか否かを識別する。人体の形状に近いときには、人体が近付いたものと判断する。そして、その部分から人体のプロポーションを割り出して顔の輪郭を識別する。

【００２５】またカメラ３は、周囲の動画データを採取して、採取した周囲の動画データの中から背景と遠近やコントラストが違う物体が写っている部分、またはあらかじめ記録されている初期状態のデータと遠近やコントラストが違う物体が写っている部分を検知する。このような部分を検知すると、その部分の形状と人体の形状とを比較して、人体の形状に近いか否かを識別する。人体の形状に近いときには、人体が近付いたものと判断する。そして、その部分から人体のプロポーションを割り出して顔の輪郭を識別する。

【００２６】以上のように構成とすることによって、カメラ３は、近接センサ２の機能である取扱者が近付いたことを検知する機能と取扱者の顔の輪郭を識別する機能を兼ね備えることができる。その結果、ＡＴＭ１の構成は、カメラ３によって近接センサ２が代用され、近接センサ２がない構成にすることができる。

【００２７】表示入力部４は、情報を表示するディスプレーであるとともに、取扱者によって各種取引処理の指示が入力されるキーである。表示入力部４は、ディスプレーの表示を制御する表示制御部１３と、キーの入力を制御・検知する入力制御部１４を有している。特に表示制御部１３は、後述するように表示制御部１３を暗く表示させたり、元に戻させたり、「サングラスを外して下さい」などの表示をさせたりする。

【００２８】紙幣挿入・排出口５は紙幣を挿入・排出する開口である。紙幣挿入・排出口５は紙幣取扱部１５と連結しており、紙幣挿入・排出口５からＡＴＭ１内に挿入された紙幣は紙幣取扱部１５によって鑑別・収納される。また、収納された紙幣は紙幣取扱部１５によって紙幣挿入・排出口５からＡＴＭ１外へ排出される。

【００２９】カード挿入・排出口６はカード２２を挿入・排出する開口である。カード挿入・排出口６はカード取扱部１６と連結しており、カード挿入・排出口６からＡＴＭ１内に挿入されたカード２２はカード取扱部１６によって取引処理に必要な主々の情報が読み取られる。

【００３０】伝票排出口７は伝票を排出する開口である。伝票排出口７は伝票取扱部１７と連結しており、伝票取扱部１７は取引処理に際して主々の情報を記載した伝票を作成する。この伝票取扱部１７によって作成された伝票は伝票排出口７からＡＴＭ１外へ排出されて取扱者の手に渡る。

【００３１】通帳挿入・排出口８は通帳を挿入・排出する開口である。通帳挿入・排出口８は通帳取扱部１８と連結しており、通帳挿入・排出口８からＡＴＭ１内に挿入された通帳は通帳取扱部１８によって実行された取引処理の内容が記録される。

【００３２】照明部９は蛍光灯や白色灯などの明りである。照明部９は、取扱者を照らして取扱者の顔・目をカメラ３の採取感度以上の照度にする。これによって、例えばＡＴＭ１に逆光が入る場合であっても、ＡＴＭ１は取扱者の顔・目のデータを良好に採取することができる。照明部９は、目に光が反射して白く輝く部分を形成しないようにする。そのため、例えば半透明なスクリーンを透過させる構成とし、間接的な明りを取扱者を照らすようにする。

【００３３】主制御部１９はＡＴＭ１の取引処理に関する種々の動作を制御する制御部であり、例えば接客動作やホストコンピュータとの通信動作などを制御する。

【００３４】主記録部２０は取引処理に関する種々の情報を記録する記録部であり、例えば銀行番号や支店番号、ＡＴＭ番号、顧客の虹彩データ（特に、ブラックリストのような特定の顧客の虹彩データ）、取引処理用のプログラムなどが記録されている。

【００３５】取引データ記録部２１は実行された取引処理の内容を記録する記録部である。この取引データ記録部２１はハードディスクやフロッピーディスク、メモリーチップ、記録紙などの形態がある。

【００３６】以下に、ＡＴＭ１の取引処理方法を説明し、これをもって本発明の虹彩データを用いた個人識別方法も説明する。

【００３７】虹彩データの用い方は以下の２通りがある。

【００３８】第１の用い方は、取引処理に際して暗証番

号に代わって虹彩データによる個人識別を行うことである。

【００３９】第２の用い方は、取引処理に際して虹彩データを用いた個人識別を行わない代わりに、暗証番号を用いた個人識別を行うとともに、取扱者の虹彩データを記録することである。この用い方は、後日、その取引処理が顧客以外の第三者による取引処理（以下、不正な取引処理と称する）などであったことが判明した場合に、取扱者の虹彩データと顧客自身の虹彩データとを比較し、事後解析などに使用する。

【００４０】第１の用い方は、高いセキュリティを要求される取引処理ができるという利点がある。高いセキュリティを要求される取引処理とは、例えば高額な取引処理や、取扱者が暗証番号を失念した場合の取引処理などである。また第１の用い方は、天災などでカードや通帳、印鑑などが消失した場合に、虹彩データを用いて、カードや通帳、印鑑がない状態で顧客確認を行って取引処理を行うことができるという利点がある。例えばカードや通帳、印鑑などを消失した顧客は端末装置（ＡＴＭ１や図示しない窓口取引装置など）に顧客データ（氏名や生年月日、住所、電話番号など）を入力するとともに、端末装置に目のデータを採取させる。端末装置は顧客の目のデータから虹彩データを抽出して、その虹彩データを虹彩データを用いた個人識別機能を有する装置（ホストコンピュータ１１やその他の図示しない装置）に送信する。虹彩データを用いた個人識別機能を有する装置はその虹彩データを用いて顧客自身であるのか否かを確認する。このように構成することによって、顧客はカードや通帳、印鑑などがない状態でも自分の口座にアクセスして取引処理をすることができる。また新たなカードや通帳も発行することができる。

【００４１】第２の用い方は、不正な取引処理が発生した場合に、その取引処理が顧客自身によらない取引処理であることを証明して顧客の信用を保全できるという利点や、その取扱者が次に取引処理をするときに検知して警報システム（図示せず）を作動させるという利点がある。

【００４２】以下に、図４および図５を用いてこれらの用い方を説明する。

【００４３】なお、ＡＴＭ１は虹彩データを採取できない場合がある。例えば、取扱者がサングラスしていたり、眼帯をしている場合である。取扱者がサングラスをしている場合は、取扱者が不審人物である可能性があるし、また虹彩データを用いた個人識別ができないので高いセキュリティーを要する取引処理ができない。そこでサングラスを外すように仕向ける必要がある。例えば、ディスプレー（表示入力部４）を暗くすることにより取扱者が無意識にサングラスを外すように仕向けることができる。また表示入力部４に「おそれいりますがサングラスを外して下さい」などを表示して取扱者が積極的に外すように仕向けることもできる。取扱者が眼帯をしている場合は、取扱者が不審人物である可能性は少ない。そこで暗証番号による取引処理は行い得るものとし、その代わり、高いセキュリティを必要とする取引処理はできないものとする。そして眼帯がされていない方の目の虹彩データを取引データ記録部２１に記憶しておき、万一、不正な取引処理が発生した場合に、その取引処理が顧客自身によらない取引処理であることを証明する。これによって顧客の信用を保全し、顧客に高いセキュリティを保証する。図４および図５のフローチャートはこれらを意図して成されたものである。

【００４４】またＡＴＭ１は、採取する虹彩データを、両目とも採取するように設定できるし、片目だけを採取するようにも設定できる。虹彩データを両目とも採取する場合は、個人識別能力を高くできるが、その反面、ホストコンピュータ１１の記憶容量を大きくする必要がある。他方、虹彩データを片目だけ採取する場合は、虹彩データを個人識別能力が小さくなるものの、ホストコンピュータ１１の記憶容量を小さくできる。本実施例では、通常は片目の虹彩データを採取するだけとし、所定の条件がある場合にのみ他方の目の虹彩データを採取して記憶するものとする。このようにすることにより、ホストコンピュータ１１の記憶容量が小さくても運用できるとともに、万一、不正な取引処理が発生した場合でも高いセキュリティを保証することができる。図４および図５のフローチャートはこれをも意図して成されたものである。

【００４５】まず第１の用い方を図４のフローチャートを用いて説明する。なお、図４のフローチャートは、図１のようにカメラ３がＡＴＭ１の前面に配設されている例に適するように組まれている。

【００４６】（ステップ１０１）ＡＴＭ１は、まず取扱者が近付いたことを近接センサ２によって検知して、取扱者の顔の輪郭を識別し、取扱者の目の位置を割り出す。次に取扱者の顔にカメラ３の焦点を合わせて取扱者の顔・目のデータを採取する。採取した取扱者の顔・目のデータが暗い場合には、カメラ３の採取感度を虹彩データを識別できるレベルまで上げて採取する。

【００４７】（ステップ１０２）ＡＴＭ１は表示入力部４の表示を開始する。

【００４８】（ステップ１０３）ＡＴＭ１は取扱者がサングラスをしているのか否かを識別する。サングラスの識別は、採取した取扱者の顔・目のデータから両目の瞳が識別できるのか否かによってなされる。瞳の識別は、取扱者の顔・目のデータから所定のスライスレベルで両目の位置に色の濃淡が明確に切り分けられる境目を検出できのるか否かによってなされる。境目を検出できた場合は瞳を識別できたものとして扱い、検出できなかった場合は瞳を識別できたものとして扱う。このようにして両目の瞳とも識別できた場合は裸眼の状態として扱い、

片方の瞳だけが識別できた場合は眼帯をしている状態として扱い、両目の瞳とも検出できなかった場合はサングラスをしている状態として扱う。なお、通常の透明な眼鏡または薄い着色のサングラスは光彩データを抽出することができる。そのため本実施例では特にこれらも識別することはしないものとした。以下、取扱者がサングラスをしている場合はステップ１０４に進み、していない場合はステップ１０９に進む。

【００４９】（ステップ１０４）ＡＴＭ１は表示入力部４を暗くする。これによって、取扱者に抵抗感を与えることなく、取扱者自身にサングラスを外させる。このようにすることによって、ＡＴＭ１は取扱者の虹彩データを良好に抽出することができるとともに、店内に設置している監視カメラ（図示せず）は取扱者の素顔を写すことができる。

【００５０】（ステップ１０５、１０６）ＡＴＭ１は所定の時間が経過するまで待機する。そして所定時間経過した後、再度、取扱者がサングラスをしているのか否かを識別する。以下、取扱者がサングラスをしている場合はステップ１０７に進み、していない場合はステップ１０８に進む。

【００５１】（ステップ１０７）ＡＴＭ１は「サングラスを外した状態でやり直して下さい」を表示入力部４に表示する。これによって犯罪を犯そうとする人物に抵抗感を与えて、犯罪を積極的に抑止する。以下、ステップ１２１に進む。

【００５２】（ステップ１０８）ＡＴＭ１は表示入力部４を明るくする（元の状態に戻す）。

【００５３】（ステップ１０９）ＡＴＭ１は、「カードを挿入して下さい」を表示入力部４に表示し、取扱者にカード２２の挿入を促す。取扱者がカード２２をカード挿入・排出口６に挿入すると、ＡＴＭ１はカード２２をＡＴＭ１内に導入してカード取扱部１６によってカード２２の情報を読み取る。

【００５４】（ステップ１１０）ＡＴＭ１は虹彩データを用いた個人識別を行うのか否かをカード２２に記録されている情報に基づいて選択する。カード２２の情報の中に虹彩データを用いた個人識別を行うことを指定する信号が記録されている場合には、ＡＴＭ１は虹彩データを用いた個人識別を行う。また、虹彩データを用いた個人識別を行わないことを指定する信号が記録されている場合には、ＡＴＭ１は虹彩データを用いた個人識別を行わずに暗証番号を用いた個人識別を行う。この虹彩データを用いた個人識別を行うのか否かを指定する信号は、カード２２ではなく、ホストコンピュータ１１に記録されていて、ホストコンピュータ１１からオンラインでＡＴＭ１に送信されるようにすることもできる。以下、この信号が虹彩データを用いた個人識別を行うことを指定する場合はステップ１１１に進み、指定しない場合はステップ１２２に進む。

【００５５】なお、カード２２の情報の中に虹彩データを用いた個人識別を行うのか否かを指定する信号が記録されていない場合は、金融機関が虹彩データを用いた個人識別を行うのか否かをあらかじめ選択して設定した個人識別を行う。

【００５６】（ステップ１１１）ＡＴＭ１は、カメラ３の焦点を取扱者の顔・目に合わせて取扱者の顔・目のデータを採取する。次にＡＴＭ１は、カメラ制御部１２（または主制御部１９）によって取扱者の顔・目のデータから取扱者の虹彩データを抽出する。この取扱者の虹彩データは、あらかじめ金融機関に登録されている方の目（所定の方の目）である。どちらが所定の方の目であるのかを指定する情報は、カード２２に記録されており、ＡＴＭ１はカード２２からこの情報を得て、所定の方の眼を特定して虹彩データを抽出する。なお、この情報はホストコンピュータ１１に記録されており、ＡＴＭ１はホストコンピュータ１１からこの情報を得て、所定の方の眼を特定して虹彩データを抽出する構成とすることも可能である。

【００５７】（ステップ１１２）ＡＴＭ１は取扱者の虹彩データを抽出できたのか否かを識別する。以下、取扱者の虹彩データを抽出できた場合はステップ１１３に進み、抽出できなかった場合はステップ１１５に進む。

【００５８】なお、上述したように取扱者が眼帯をしている場合には、虹彩データが抽出できない。この場合は、サングラスの場合と異なり、取扱者が不審人物である可能性は低い。そこで高いセキュリティーを必要とする取引処理はできない代わりに、暗証番号を用いた個人識別による取引処理は行い得るものとする。そして眼帯がされていない方の目の虹彩データを抽出して取引データ記録部２１に記憶しておき、後日、その取引処理が不正な取引処理であったことが判明した場合に、虹彩データを用いた個人識別機能を有する装置（ホストコンピュータ１１やその他の図示しない窓口取引装置など）によって取扱者の虹彩データと顧客の虹彩データとを比較して、その取引処理が顧客自身によらない取引処理であることを証明し、もって顧客の信用を保全する。

【００５９】（ステップ１１３）ＡＴＭ１は取扱者の虹彩データとカード２２の情報の中に記録されている顧客の虹彩データを比較する。顧客の虹彩データとは、あらかじめ金融機関に登録されている顧客の虹彩データである。顧客の虹彩データは、複数の人物のデータを１グループの顧客として記録することができる。例えば顧客が法人の場合には、法人の代表者とその代理人などを１グループの顧客として記録する。このようにすることによって、このグループの中の誰かが取扱者である場合には取引処理が実行できる。

【００６０】上述の比較によって両者が一致する場合には、ＡＴＭ１は、取扱者が顧客自身であると見なして取引処理を行い得る状態になる。以下、ステップ１１４に

進む。一方、両者が一致しない場合は、ステップ１１６に進む。

【００６１】（ステップ１１４）ＡＴＭ１は取扱者の虹彩データをホストコンピュータ１１にオンラインで送信する。ホストコンピュータ１１はそのデータを記録部（図示せず）に記録する。以下、ステップ１２４に進む。

【００６２】なお、ステップ１１４において取扱者の虹彩データを記録するのか否かは金融機関が選択し得る事項である。ただし、複数の人物のデータを１グループの顧客として記録している場合には記録する方が望ましい。

【００６３】（ステップ１１５）ＡＴＭ１は他方の目の虹彩データを抽出する。

【００６４】（ステップ１１６）ＡＴＭ１は「暗証番号を入力して下さい」を表示入力部４に表示する。その表示に基づいて取扱者が暗証番号を入力すると、ＡＴＭ１は暗証番号と取扱者の虹彩データをホストコンピュータ１１にオンラインで送信する。

【００６５】（ステップ１１７）ホストコンピュータ１１はＡＴＭ１から受信した暗証番号とホストコンピュータ１１自身に記録されている暗証番号を比較する。以下、両者が一致する場合はステップ１１８に進み、一致しない場合はステップ１１９に進む。

【００６６】（ステップ１１８）ホストコンピュータ１１は取扱者の虹彩データを記録する。このようにすることによって、上述の通り、後日、その取引処理が不正な取引処理であったことが判明した場合に、虹彩データを用いた個人識別機能を有する装置（ホストコンピュータ１１やその他の図示しない窓口取引装置など）によって取扱者の虹彩データと顧客の虹彩データとを比較して、その取引処理が顧客自身によらない取引処理であることを証明し、もって顧客の信用を保全する。その結果、顧客の信用に傷が付くのを防いだり、顧客の財産を保護するように保険を適用することを可能とする。また、その取扱者の虹彩データをホストコンピュータ１１の記録部のブラックリストに記録する。このブラックリストは防犯用のファイルであり、取引処理毎に照会される。このように構成することによりホストコンピュータ１１は不正な取引処理を行った実行者が次に取引処理をするときにこれを検知して警報システム（図示せず）を作動することができ、金融機関は不正な取扱者を検挙することが可能となる。なお、金融機関は不正な取引処理が行われた際に取扱者が写っているビデオテープを保管しておき、検挙に際してこのビデオテープを照会することによって検挙の正確性を高めることができる。

【００６７】（ステップ１１９）ＡＴＭ１は所定回数連続して誤った暗証番号が入力されたか否かを識別する。以下、誤った入力が所定回数未満の場合はステップ１１６に進み、所定回数以上の場合はステップ１２０に進む。

【００６８】（ステップ１２０）ＡＴＭ１は、カード２２をＡＴＭ１内の収納部（図示せず）に取り込み、「窓口に来て下さい」と記録した伝票を顧客に発行する。同時に、取扱者の虹彩データを取引データ記録部２１に記録するとともに、その虹彩データをホストコンピュータ１１に送信する。ホストコンピュータ１１はその虹彩データを記録部に記録する。記録部に記録された虹彩データは、後日、その取引処理が不正な取引処理であったことが判明した場合にブラックリストに記録される。

【００６９】（ステップ１２１）ＡＴＭ１は取引処理を不可と判断して取引処理を中断する。以下、ステップ１２７に進む。

【００７０】（ステップ１２２）ＡＴＭ１は「暗証番号を入力して下さい」を表示入力部４に表示する。その表示に基づいて取扱者が暗証番号を入力すると、ＡＴＭ１は暗証番号と取扱者の虹彩データをホストコンピュータ１１にオンラインで送信する。

【００７１】（ステップ１２３）ホストコンピュータ１１はＡＴＭ１から受信した暗証番号とホストコンピュータ１１自身に記録されている暗証番号を比較する。以下、両者が一致する場合はステップ１２４に進み、一致しない場合はステップ１２５に進む。

【００７２】（ステップ１２４）ＡＴＭ１は取引処理を可と判断して取引処理を実行する。以下、ステップ１２７に進む。

【００７３】（ステップ１２５）ＡＴＭ１は所定回数連続して誤った暗証番号が入力されたか否かを識別する。以下、誤った入力が所定回数未満の場合はステップ１２２に進み、所定回数以上の場合はステップ１２６に進む。

【００７４】（ステップ１２６）ＡＴＭ１は取引処理を不可と判断して、カード２２をＡＴＭ１内の収納部に取り込み、「窓口に来て下さい」と記録した伝票を顧客に発行して取引処理を中断する。

【００７５】（ステップ１２７）ＡＴＭ１は処理を終了する。

【００７６】なお、上述のフローチャートはＡＴＭ１が虹彩データを用いた個人識別を行うように組まれているが、カード２２が虹彩データを用いた個人識別を行うように組むこともできる。例えば、カード２２を顧客の虹彩データを記録しているＩＣカードとし、ＡＴＭ１はカード２２に取扱者の虹彩データを送信し、カード２２が受信した取扱者の虹彩データと記録している顧客の虹彩データとを比較する構成とする。カード２２をこのように構成することにより、カード２２が虹彩データを用いた個人識別を行うフローチャートを実現することができる。

【００７７】以上、第１の用い方を詳細に説明した。なお、上述の図４のフローチャートには以下のような特徴

も示されている。

【００７８】第１に、虹彩データを用いた個人識別を行うのか否かは、カード２２に記録されている虹彩データを用いた個人識別を行うことを指定する信号、または虹彩データを用いた個人識別を行わないことを指定する信号に基づいて行われる。また、カード２２の情報の中に虹彩データを用いた個人識別を行うのか否かを指定する信号が記録されていない場合は、金融機関が虹彩データを用いた個人識別を行うのか否かをあらかじめ選択して設定した個人識別を行う。

【００７９】第２に、虹彩データを用いた個人識別は、ＡＴＭ１がカード２２の情報の中に記録されている顧客の虹彩データを用いて行われている。

【００８０】第３に、取扱者の顔・目のデータからサングラスが識別された場合には、サングラスを外すように注意を喚起させている。例えば表示入力部４の輝度を変化、特に表示入力部４を暗くすることによって、取扱者に抵抗感を与えることなく取扱者自身に外させるように仕向けている。また表示入力部４に「サングラスを外した状態でやり直して下さい」と表示することによって、犯罪を犯そうとする人物に抵抗感を与えて、犯罪を積極的に抑止している。なお、注意を喚起させる手法は、この他にも音声によって「サングラスを外した状態でやり直して下さい」と発声させることもできる。

【００８１】第４に、所定の方の目の虹彩データが抽出できない場合（眼帯が識別された場合）には、虹彩データを用いた個人識別を行わずに、他方の目の虹彩データを抽出して記憶するとともに、暗証番号を用いた個人識別を行う。

【００８２】第５に、取扱者の虹彩データがカード２２に記録された顧客の虹彩データと異なる場合には、取扱者の虹彩データを記録する。

【００８３】次に第２の用い方を図５のフローチャートを用いて説明する。なお、図５のフローチャートは、図２のようにカメラ３が表示入力部４の近傍に配置されている例に適するように組まれている。

【００８４】（ステップ２０１）ＡＴＭ１は、取扱者が近付いたことを近接センサ２によって検知して、取扱者の顔の輪郭を識別し、取扱者の目の位置を割り出す。

【００８５】（ステップ２０２）ＡＴＭ１は表示入力部４の表示を開始する。表示入力部４は、輝度の高い画面を表示して取扱者の顔に明りを照らすことによって照明部９を代用している。このような構成した場合に、輝度の高い画面を取引処理中も表示し続けると取扱者に違和感を与える。そこで本発明では、取扱者が近付いたときにだけ輝度の高い画面を表示し、虹彩データが抽出されると輝度を落とすようにする方が望ましい。

【００８６】（ステップ２０３）ＡＴＭ１は、「カードを挿入して下さい」を表示入力部４に表示し、取扱者にカード２２の挿入を促す。取扱者がカード２２をカード挿入・排出口６に挿入すると、ＡＴＭ１はカード２２をＡＴＭ１内に導入してカード取扱部１６によってカード２２の情報を読み取る。

【００８７】（ステップ２０４）ＡＴＭ１は虹彩データを用いた個人識別を行うのか否かをカード２２に記録されている情報に基づいて選択する。以下、カード２２の情報の中に虹彩データを用いた個人識別を行うことを指定する信号が記録されている場合にはステップ２０５に進み、虹彩データを用いた個人識別を行わないことを指定する信号が記録されている場合にはステップ２１９に進む。

【００８８】（ステップ２０５）ＡＴＭ１は、カメラ３によって取扱者の顔・目のデータを採取して、取扱者がサングラスをしているのか否かを識別する。以下、取扱者がサングラスをしている場合はステップ２０６に進み、していない場合はステップ２１０に進む。

【００８９】（ステップ２０６）ＡＴＭ１は「サングラスを外して下さい」を表示入力部４に表示する。これによって犯罪を犯そうとする人物に抵抗感を与えて、犯罪を積極的に抑止する。

【００９０】（ステップ２０７、２０８）ＡＴＭ１は所定の時間が経過するまで待機する。そして所定時間経過した後、再度、取扱者がサングラスをしているのか否かを識別する。以下、取扱者がサングラスをしている場合はステップ２０９に進み、していない場合はステップ２１０に進む。

【００９１】（ステップ２０９）ＡＴＭ１は「サングラスを外した状態でやり直して下さい」を表示入力部４に表示する。以下、ステップ２１８に進む。

【００９２】（ステップ２１０）ＡＴＭ１は、カメラ制御部１２（または主制御部１９）によって取扱者の顔・目のデータから取扱者の虹彩データを抽出する。この取扱者の虹彩データは、所定の方の目（あらかじめ金融機関に登録されている方の目）であり、どちらが所定の方の目であるのかを指定する情報はカード２２に記録されている。

【００９３】（ステップ２１１）ＡＴＭ１は取扱者の虹彩データを抽出できたのか否かを識別する。以下、取扱者の虹彩データを抽出できた場合はステップ２１３に進み、抽出できなかった場合はステップ２１２に進む。

【００９４】（ステップ２１２）ＡＴＭ１は他方の目の虹彩データを抽出する。

【００９５】（ステップ２１３）ＡＴＭ１は「暗証番号を入力して下さい」を表示入力部４に表示する。その表示に基づいて取扱者が暗証番号を入力すると、ＡＴＭ１は暗証番号と取扱者の虹彩データをホストコンピュータ１１にオンラインで送信する。

【００９６】（ステップ２１４）ホストコンピュータ１１はＡＴＭ１から受信した暗証番号とホストコンピュータ１１自身に記録されている暗証番号を比較する。以

下、両者が一致する場合はステップ２１５に進み、一致しない場合はステップ２１６に進む。

【００９７】（ステップ２１５）ホストコンピュータ１１は取扱者の虹彩データを記録する。このステップは図４のステップ１１８と同様の効果を目的としている。

【００９８】（ステップ２１６）ＡＴＭ１は所定回数連続して誤った暗証番号が入力されたか否かを識別する。以下、誤った入力が所定回数未満の場合はステップ２１３に進み、所定回数以上の場合はステップ２１７に進む。

【００９９】（ステップ２１７）ＡＴＭ１は、カード２２をＡＴＭ１内の収納部に取り込み、「窓口に来て下さい」と記録した伝票を顧客に発行する。同時に、取扱者の虹彩データを取引データ記録部２１に記録するとともに、その虹彩データをホストコンピュータ１１に送信する。ホストコンピュータ１１はその虹彩データを記録部に記録する。記録部に記録された虹彩データは、後日、その取引処理が不正な取引処理であったことが判明した場合にブラックリストに記録される。

【０１００】（ステップ２１８）ＡＴＭ１は取引処理を不可と判断し、取引処理を中断する。以下、ステップ２２４に進む。

【０１０１】（ステップ２１９）ＡＴＭ１は「暗証番号を入力して下さい」を表示入力部４に表示する。その表示に基づいて取扱者が暗証番号を入力すると、ＡＴＭ１は暗証番号と取扱者の虹彩データをホストコンピュータ１１にオンラインで送信する。

【０１０２】（ステップ２２０）ホストコンピュータ１１はＡＴＭ１から受信した暗証番号とホストコンピュータ１１自身に記録されている暗証番号を比較する。以下、両者が一致する場合はステップ２２１に進み、一致しない場合はステップ２２２に進む。

【０１０３】（ステップ２２１）ＡＴＭ１は取引処理を可と判断して取引処理を実行する。以下、ステップ２２４に進む。

【０１０４】（ステップ２２２）ＡＴＭ１は所定回数連続して誤った暗証番号が入力されたか否かを識別する。以下、誤った入力が所定回数未満の場合はステップ２１９に進み、所定回数以上の場合はステップ２２３に進む。

【０１０５】（ステップ２２３）ＡＴＭ１は取引処理を不可と判断して、カード２２をＡＴＭ１内の収納部に取り込み、「窓口に来て下さい」と記録した伝票を顧客に発行して取引処理を中断する。

【０１０６】（ステップ２２４）ＡＴＭ１は処理を終了する。

【０１０７】以上、第２の用い方を詳細に説明した。なお、上述の図５のフローチャートには以下のような特徴も示されている。

【０１０８】第１に、ＡＴＭ１は取扱者が近付いたことを検知すると、表示入力部４に輝度の高い画面を表示して取扱者の顔に明りを照らす。これによって取扱者の顔周辺を明るくして良好なデータを得られるようにする。この画面表示は、取扱者が近付いたときにだけ輝度の高い画面を表示し、虹彩データが抽出されると輝度を落とすようにする。

【０１０９】第２に、表示入力部４の近傍にカメラ３が配設されたＡＴＭ１が取扱者の顔・目のデータを採取しやすいように、フローチャートを、取扱者がカード２２をカード挿入・排出口６に挿入して表示入力部４に視線を注視しているときに顔・目のデータを採取するようにしている。

【０１１０】第３に、暗証番号を用いた個人識別を行うまでの工程を少なくするために、取扱者がサングラスをしているか否かを識別する工程を、取扱者がカード２２を挿入する工程の後とした（または暗証番号を用いた個人識別を行う場合は除外した）。

【０１１１】

【発明の効果】第１および第２および第３および第４の発明は、サングラス識別手段（主制御部１９）によって取扱者がサングラスをしているのか否かを識別するので、不審人物を排除することができるし、不正な取引処理を防止することもできる。また第２および第３の発明は、取扱者に抵抗感を与えることなくサングラスを外させることができるので、不審人物である可能性が高い人物のデータを記録することができる。さらに第４の発明は、犯罪を犯そうとする人物に抵抗感を与えるので、犯罪を積極的に抑止することができる。

【０１１２】第５の発明は、眼帯識別手段（主制御部１９）によって取扱者が眼帯をしているのか否かを識別するので、眼帯をしている場合には、セキュリティーの高い取引処理はすることができないものの、セキュリティーの低い取引処理はすることができる。またセキュリティーの低い取引処理を行った際に取扱者のデータを記録しているので、万一、その取引処理が不正な取引処理であることが判明した場合に、その取引処理が顧客自身によらない取引処理であることを証明することができる。そのため、顧客の信用を保全することが可能となる。

【０１１３】第６の発明は、第１の発明と同様に、取扱者がサングラスをしているのか否かを識別するので、不審人物を排除することができるし、不正な取引処理を防止することもできる。

【０１１４】第７および第８の発明は、第２および第３の発明と同様に、取扱者に抵抗感を与えることなくサングラスを外させることができるので、不審人物である可能性が高い人物のデータを記録することができる。

【０１１５】第９の発明は、第４の発明と同様に、犯罪を犯そうとする人物に抵抗感を与えるので、犯罪を積極的に抑止することができる。

【０１１６】第１０の発明は、第５の発明と同様に、取

扱者が眼帯をしているのか否かを識別するので、眼帯をしている場合には、セキュリティーの高い取引処理はすることができないものの、セキュリティーの低い取引処理はすることができる。またセキュリティーの低い取引処理を行った際に取扱者のデータを記録しているので、万一、その取引処理が不正な取引処理であることが判明した場合に、その取引処理が顧客自身によらない取引処理であることを証明することができる。そのため、顧客の信用を保全することが可能となる。虹彩データを用いた個人識別によらない取引処理を行う場合には、セキュリティーの高い取引処理はすることができないものの、セキュリティーの低い取引処理はすることができる。また取扱者の虹彩データを記録しているので、万一、その取引処理が不正な取引処理であることが判明した場合に、その取引処理が顧客自身によらない取引処理であることを証明することができる。

【図面の簡単な説明】

【図１】本発明に係る金融端末装置の一例を示す図である。

【図２】本発明に係る金融端末装置の他の例を示す図である。

【図３】本発明に係る金融端末装置の内部ブロックを示す図である。

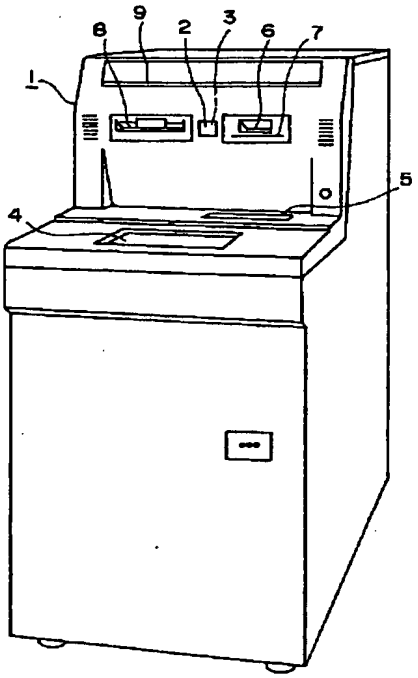
【図４】本発明の第１の用い方を示すフローチャートである。

【図５】本発明の第２の用い方を示すフローチャートである。

【符号の説明】

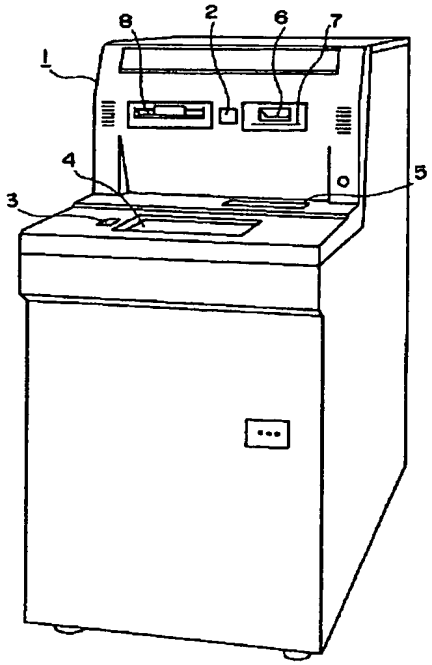
１　金融端末装置（ＡＴＭ）
２　近接センサ
３　カメラ
４　表示入力部
６　カード挿入・排出口
９　照明部
１１　ホストコンピュータ
１２　カメラ制御部
１３　表示制御部
１６　カード取扱部
１９　主制御部
２０　主記録部
２１　取引データ記録部
２２　カード

【図１】



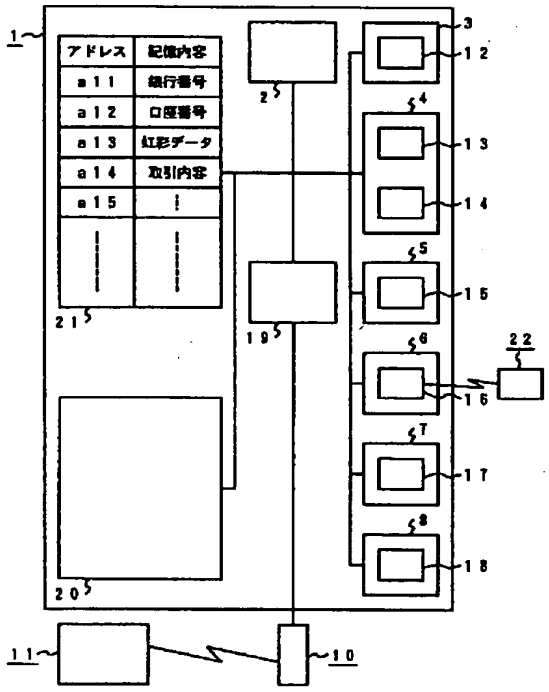
本発明に係る金融端末装置の一例を示す図

【図２】



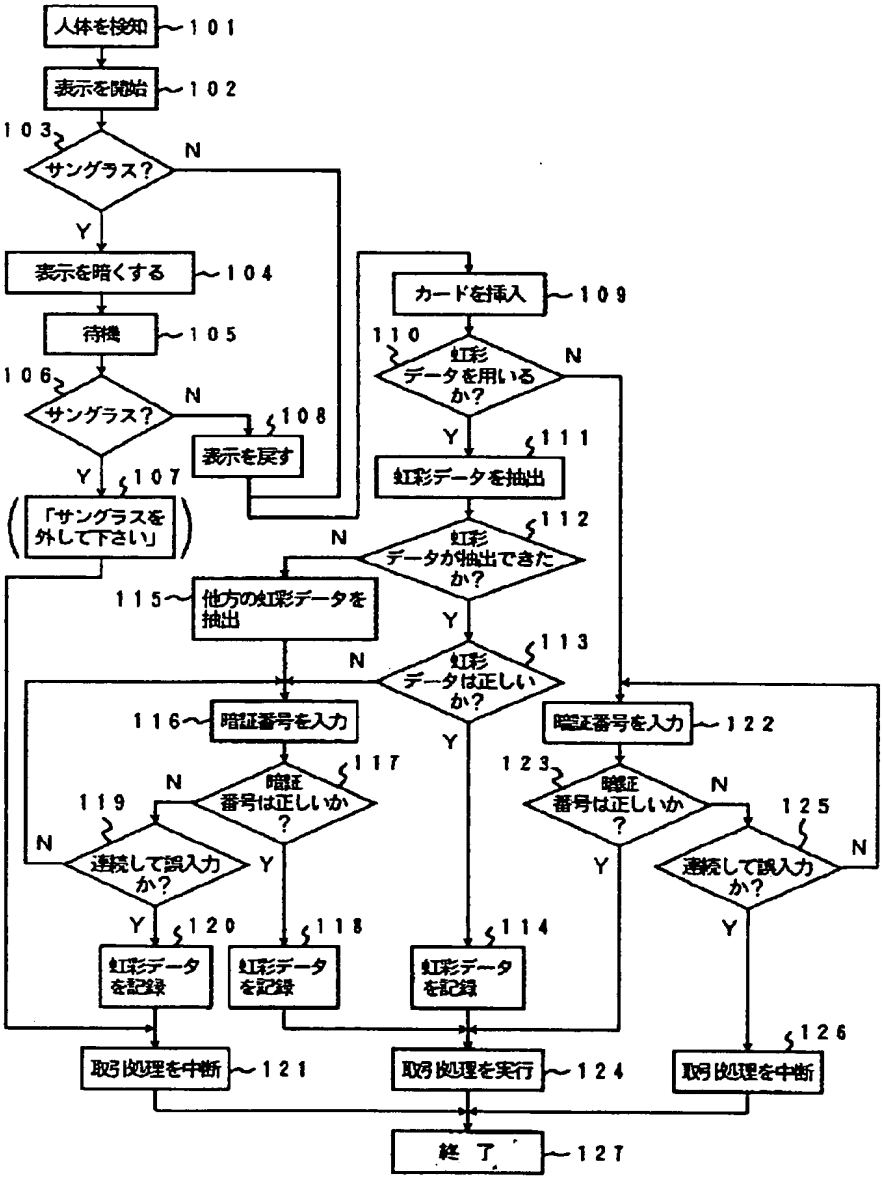
本発明に係る金融端末装置の他の例を示す図

【図３】



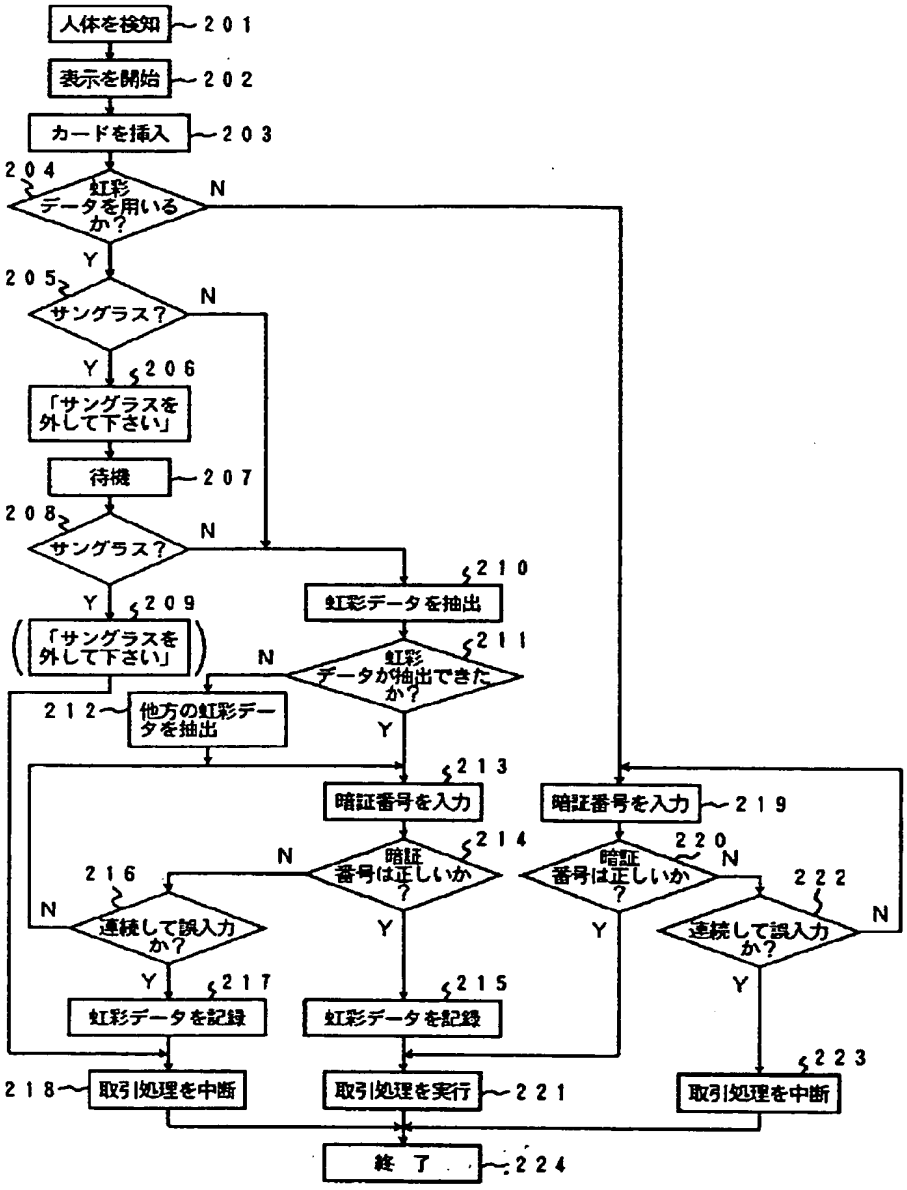
本発明に係る金融端末装置の内部ブロックを示す図

【図４】



本発明の第１の用い方を示すフローチャート

【図５】



本発明の第２の用い方を示すフローチャート